

IMPLEMENTASI ALGORITMA RC4 DAN CIPHER BLOCK CHAINING (CBC) PADA PENGAMANAN GAMBAR

ALVIAN YUDHA PRAWIRA

(Pembimbing : T. Sutojo, S.Si, M.Kom)

Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro

www.dinus.ac.id

Email : 111201207112@mhs.dinus.ac.id

ABSTRAK

File berbentuk gambar saat ini digunakan sebagai media informasi yang dianggap sangat akurat karena dapat mewakili kebenaran suatu informasi penting. Maraknya penyadapan, pencurian, serta penyalahgunaan data gambar biasanya di gunakan untuk menjatuhkan seseorang bahkan sebuah kelompok, oleh sebab itu muncul ide membuat sistem keamanan data dengan algoritma kriptografi dengan mengimplementasikan algoritma RC4 dan CBC untuk merahasiakan data dengan format gambar. Berdasarkan hasil perancangan, pembuatan, dan pengujian aplikasi pengamanan citra digital menggunakan algoritma RC4 dan Chiper Block Chaining (CBC), dapat di tarik kesimpulan yaitu: Algoritma RC4 dan Chiper Block Chaining dapat di gunakan untuk mengamankan file citra digital. Hasil dari proses enkripsi dengan mengimplementasikan Algoritma RC4 dan Chiper Block Chaining (CBC) sulit di mengerti secara visual. Berdasarkan pengujian, dekripsi menghasilkan gambar yang masih sama atau dapat kembali seperti gambar asli, namun pada perhitungan MSE dan PSNR perbandingan gambar asli (plaintext) dengan hasil enkripsi dan dekripsi tidak sama 100% karena hasil yang di peroleh tidak 0 sebab selama proses enkripsi pasti ada sebagian kecil data yang rusak, menyebabkan terjadi perbedaan pada ukuran file. untuk penelitian selanjutnya perlu di lakukan pengembangan pada kecepatan dan penyempurnaan pada perbandingan gambar asli dan hasil dekripsi.

Kata Kunci : RC4, CBC, keamanan, gambar,citra,kriptografi

IMPLEMENTATION OF RC4 AND CIPHER BLOCK CHAINING (CBC) FOR IMAGE SECURITY

ALVIAN YUDHA PRAWIRA

(Lecturer : T. Sutojo, S.Si, M.Kom)

*Bachelor of Informatics Engineering - S1, Faculty of Computer
Science, DINUS University*

www.dinus.ac.id

Email : 111201207112 @mhs.dinus.ac.id

ABSTRACT

A file-shaped image is currently used as a medium of information that is considered to be very accurate because it can represent the truth of the important information. Rampant wiretapping, theft, and misuse of the image data are usually used to drop someone even a group, hence came the idea to create a system of data security by implementing a cryptographic algorithm RC4 algorithm and CBC to keep the data in a picture format. Based on the results of the design, manufacture, and testing of digital image security applications using the RC4 algorithm and Cipher Block Chaining (CBC), it can be deduced that: RC4 algorithm and Cipher Block Chaining mode can be used to secure the digital image file. The results of the process of implementing encryption with the RC4 algorithm and Cipher Block Chaining (CBC) is difficult to understand visually. Based on testing, decryption produces an image that is still the same or can be returned to the original image, but in the calculation of MSE and PSNR comparison of the original image (plaintext) with the results of the encryption and decryption does not equal 100% due to the results obtained is not 0 because during the encryption process must be a small portion of data that is damaged, causing a difference in the size of the file. for further research needs to be done on the speed of development and improvement in the ratio of the original image and the result of decryption.

Keyword : RC4,CBC,security, image, cryptography